CLAIMS

What is claimed is:

1

1   1.   A method for detecting an unwanted message, comprising:

2   (a)   receiving an electronic mail message;

3   (b)   decomposing text in the electronic mail message;

4   (c)   gathering statistics associated with the text using a statistical analyzer; and

5   (d)   analyzing the statistics for determining whether the electronic mail message is an

6   unwanted message.

1

1   2.   The method as recited in claim 1, wherein the statistics gathered using the

2   statistical analyzer include a ratio of words capitalized to total number of words.

1

1   3.   The method as recited in claim 1, wherein the statistics gathered using the

2   statistical analyzer include a punctuation to word ratio.

1   4.   The method as recited in claim 1, wherein the statistics gathered using the

2   statistical analyzer include a number of uniform resource locators (URLs) in the

3   text.

1   5.   The method as recited in claim 1, wherein the statistics gathered using the

2   statistical analyzer include at least one telephone number in the text.

1   6.   The method as recited in claim 1, wherein the statistics gathered using the

2   statistical analyzer include results of an analysis of character type.

1 7. The method as recited in claim 1, wherein the statistics gathered using the
2 statistical analyzer include results of an analysis of a URL in the text.

1 8. The method as recited in claim 1, wherein the statistics gathered using the
2 statistical analyzer include results of an analysis of e-mail addresses in the text.

1 9. The method as recited in claim 1, wherein the statistics gathered using the
2 statistical analyzer include results of a message header field analysis.

1 10. The method as recited in claim 1, wherein the statistics gathered using the
2 statistical analyzer include a ratio of words capitalized to total number of words,
3 a punctuation to word ratio, a number of URLs in the text, a number of
4 telephone numbers in the text, addresses in the text, and results of a message
5 header field analysis.

1 11. The method as recited in claim 1, wherein the statistics are placed in a results
2 table, wherein entries in the table are passed as inputs to a neural network
3 engine.

1 12. The method as recited in claim 1, wherein the statistics are sent to a neural
2 network engine, wherein the neural network engine compares the statistics to
3 predetermined weights for determining whether the electronic mail message is
4 an unwanted message.

1 13. The method as recited in claim 12, wherein the neural network engine is taught
2 to recognize unwanted messages.

1   14.   The method as recited in claim 13, wherein examples are provided to the neural
2   network engine, wherein the examples are of wanted messages and unwanted
3   messages, and each of the examples is associated with a desired output.

1   15.   The method as recited in claim 14, wherein each of the examples are processed
2   with statistics by the neural network engine for generating weights for the
3   statistics, wherein each of the weights is used to denote wanted and unwanted
4   messages.

1   16.   The method as recited in claim 15, wherein the neural network engine utilizes
2   adaptive linear combination for adjusting the weights.

1   17.   The method as recited in claim 15, wherein logic associated with the neural
2   network engine is updated based on the processing by the neural network engine.

1   18.   The method as recited in claim 17, wherein the neural network engine is updated
2   to recognize an unwanted message, the message is identified as an unwanted
3   message, the features of the message that make the message unwanted are
4   identified, and the identified features are stored and used by the neural network
5   to identify subsequent unwanted messages.
1

1   19.   The method as recited in claim 1, wherein the neural network engine analyzes
2   previous user input for determining whether the message is unwanted.
1

1   20.   A computer program product for detecting an unwanted message, comprising:
2   (a)   computer code for receiving an electronic mail message;
3   (b)   computer code for decomposing text in the electronic mail message;

4   (c)   computer code for gathering statistics associated with the text using a statistical

5   analyzer; and

6   (d)   computer code for analyzing the statistics for determining whether the electronic

7   mail message is an unwanted message.

1   21.   A system for detecting an unwanted message, comprising:

2   (a)   a statistical analyzer for gathering statistics associated with text retrieved from

3   an electronic mail message; and

4   (b)   a neural network engine coupled to the statistical analyzer for analyzing the

5   statistics;

6   (c)   wherein the neural network engine determines whether the electronic mail

7   message is an unwanted message.

1   22.   A method for detecting an unwanted message, comprising:

2   (a)   receiving an electronic mail message;

3   (b)   decomposing text in the electronic mail message;

4   (c)   gathering statistics associated with the text using a statistical analyzer, wherein

5   the statistics gathered using the statistical analyzer include at least three of a

6   ratio of words capitalized to total number of words, a punctuation to word ratio,

7   a number of URLs in the text, a telephone number in the text, results of an

8   analysis of a URL in the text, results of an analysis of e-mail addresses in the

9   text, results of an analysis of character type, and results of a message header

10   field analysis; and

11   (d)   analyzing the statistics for determining whether the electronic mail message is an

12   unwanted message.

1